8f

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/588,049 | 06/06/2000 | MASAKI KYOJIMA | 106406 | 8128 |

25944 7590 02/20/2004

OLIFF & BERRIDGE, PLC
P.O. BOX 19928
ALEXANDRIA, VA 22320

| EXAMINER | |
|---|---|
| LANIER, BENJAMIN E | |
| ART UNIT | PAPER NUMBER |
| 2132 | 5 |

DATE MAILED: 02/20/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

8f

|  |  |  |  |
|---|---|---|---|
| *Office Action Summary* | **Application No.**<br>09/588,049 | **Applicant(s)**<br>KYOJIMA ET AL. |  |
|  | **Examiner**<br>Benjamin E Lanier | **Art Unit**<br>2132 |  |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE ____ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 June 2000* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. §§ 119 and 120**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 3 .

4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: .

## DETAILED ACTION

### *Claim Rejections - 35 USC § 102*

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-4, 6, 8-13, 15, 17-22, 24-27, 29-32 are rejected under 35 U.S.C. 102(b) as being anticipated by Boebert, U.S. Patent No. 5,502,766. Referring to claims 1, 3, 8-10, 12, 17-20, 22, 26, 27, 29-32, Boebert discloses a data enclave system wherein a workstation user's ID and PIN, stored in the memory of their Personal Keying Device (data-for-second-checking memory unit), is used to generate an encryption key (Col. 10, lines 22-34), which meets the limitation key generation unit for generating an encrypting key from data stored in the data-for-secondary-checking memory unit. The generated encryption key is the used to encrypted the access vector and media key that is stored in the storage search logic (data-for-main-checking memory unit)(Col. 13, lines 42-57), which meets the limitation of an encryptor for encrypting data stored in the data-for-main-checking memory unit with the encrypting key generated by the encrypting key generation unit. Authentication protocols are executed with the use of two pseudo random number sequences (Col. 26, lines 44-47). The enciphered Media key and access vector pair arrives at the Crypto Media Controller and the Media ID is used as an index to store the enciphered pair packet in the Personal Keying Device of the user. The media can now be identified and the individual Personal Keying Device contains a media key which can only be used by someone who has physical possession of that Personal Keying Device, knows that

individuals PIN, and has the Media of controlled by a Crypto Media Controller containing the enclave key (Col. 13, line 64 – Col. 14, line 13), which meets the limitations of the data verification between units.

Referring to claims 2, 6, 11, 15, 21, 24, 25, Boebert discloses that keys can be stored in a database (key memory) for later use (Col. 26, lines 8-13).

Referring to claim 4, 13, Boebert discloses that digital signatures can be used in the data enclave system (Col. 23, lines 50-53).

### *Claim Rejections - 35 USC § 103*

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 5, 7, 14, 16, 23, 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boebert, U.S. Patent No. 5,502,766, in view of Misra, U.S. Patent No. 5,757,920. Referring to claims 5, 7, 14, 16, 23, 28, Boebert discloses a data enclave system wherein a workstation user's ID and PIN, stored in the memory of their Personal Keying Device (data-for-second-checking memory unit), is used to generate an encryption key (Col. 10, lines 22-34), which meets the limitation key generation unit for generating an encrypting key from data stored in the data-for-secondary-checking memory unit. The generated encryption key is the used to encrypted the access vector and media key that is stored in the storage search logic (data-for-main-checking memory unit)(Col. 13, lines 42-57), which meets the limitation of an encryptor for encrypting data stored in the data-for-main-checking memory unit with the encrypting key generated by the

encrypting key generation unit. Authentication protocols are executed with the use of two pseudo random number sequences (Col. 26, lines 44-47). The enciphered Media key and access vector pair arrives at the Crypto Media Controller and the Media ID is used as an index to store the enciphered pair packet in the Personal Keying Device of the user. The media can now be identified and the individual Personal Keying Device contains a media key which can only be used by someone who has physical possession of that Personal Keying Device, knows that individuals PIN, and has the Media of controlled by a Crypto Media Controller containing the enclave key (Col. 13, line 64 – Col. 14, line 13), which meets the limitations of the data verification between units. Boebert does not disclose using symmetric key algorithms of one-way hash functions to generate encryption keys. Misra discloses a logon certification system wherein user/machines attempt to connect to a system using logon certificates. The logon certificates can be created using symmetric encryption (Col. 5, lines 22-30). Encryption keys are generated for the logon certificates using a one way hash function of the user password (Col. 6, line 63 – Col. 7, line 6). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use symmetric encryption and one way hash functions in the data enclave system of Boebert because Misra discloses that symmetric encryption is a known method in the art (Col. 5, lines 22-30) and that using one way hash function of a user password to generate encryption keys helps prevent from fraudulent logins as taught in Misra (Col. 7, lines 4-6).

## *Conclusion*

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E Lanier whose telephone number is 703-305-7684. The examiner can normally be reached on M-Th0 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703)305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-746-7239.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Benjamin E. Lanier

Gilberto

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100